

Privacy Policy

Notch Above Bookkeeping Pty Ltd

ABN 29 169 688 966

Registered BAS Agent No. 25910588

Version: 1.0

Last Updated: 1 October 2026

1. Purpose of this Privacy Policy

Notch Above Bookkeeping Pty Ltd ("Notch Above", "we", "us" or "our") respects your privacy and is committed to protecting personal information.

This Privacy Policy explains how we collect, hold, use, disclose and protect personal information in connection with our bookkeeping, BAS, payroll, accounting technology support, advisory and related services.

We are committed to handling personal information in accordance with the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Notifiable Data Breaches Scheme and our professional obligations as a registered BAS Agent.

By engaging our services, visiting our website or otherwise interacting with us, you acknowledge that your personal information may be handled in accordance with this Privacy Policy.

2. Who We Are

Notch Above provides bookkeeping, BAS, payroll, accounts payable, accounts receivable, software implementation, software training, management reporting, advisory and related business support services to Australian businesses.

As a registered BAS Agent, we are also bound by confidentiality obligations under the Tax Agent Services Act 2009 (Cth) and the Tax Practitioners Board Code of Professional Conduct.

2A. Definitions

For the purposes of this Privacy Policy:

Personal Information has the meaning given in the Privacy Act 1988 (Cth) and generally means information or an opinion about an identified individual, or an individual who is reasonably identifiable.

Sensitive Information has the meaning given in the Privacy Act 1988 (Cth) and includes information such as health information, biometric information and certain other categories of personal information requiring additional protection.

Client includes our current, former and prospective clients, together with their directors, shareholders, employees, authorised representatives and other individuals whose personal information is provided to us in connection with the services we provide.

3. What Personal Information We Collect

The personal information we collect depends on the services we provide.

Information may include:

Contact Information

- Name
- Business name
- Position or role
- Postal address
- Email address
- Telephone number

Business and Financial Information

- Director information
- Shareholder information
- Trust information
- Beneficiary information
- Business financial records
- Banking information
- Supplier information
- Customer information
- Transaction records
- Tax and BAS-related information

Payroll and Employment Information

Where we provide payroll services, information may include:

- Employee names
- Contact details
- Dates of birth
- Tax File Numbers (TFNs)
- Bank account details
- Superannuation information
- Payroll records
- Leave records
- Employment-related information required for payroll administration

Communications Information

- Emails
- Meeting notes
- Telephone records
- Client instructions
- Service requests
- Correspondence and communications

Information We Generally Do Not Collect

We generally do not collect or retain copies of identity documents such as passports, driver licences or Medicare cards.

Where identity verification is required, this is typically completed through approved third-party onboarding and verification providers.

We do not routinely seek sensitive information. Where we need to collect it, we do so with the individual's consent and only where reasonably necessary for our services, unless collection is otherwise required or permitted by law.

4. How We Collect Personal Information

We generally collect information directly from:

- Clients
- Client representatives
- Directors, shareholders and business owners
- Employees of our clients
- Authorised contacts

Information may be collected through:

- Email communications
- Telephone conversations
- Video meetings
- Microsoft Teams
- Client onboarding processes
- Ignition
- Xero
- Hubdoc
- Dext
- Employment Hero
- Deputy
- Tanda
- Karbon
- Microsoft 365 applications
- Dropbox
- SharePoint
- Other systems authorised by our clients

We may also receive information from third parties where authorised by the client or permitted by law.

5. Why We Collect Personal Information

We collect, hold and use personal information to:

- Deliver bookkeeping and BAS services
- Process payroll and superannuation obligations
- Manage accounts payable and receivable functions

- Maintain client records
- Communicate with clients
- Provide software support and implementation services
- Meet bookkeeping, payroll, BAS Agent, superannuation and other applicable legal, regulatory and professional obligations
- Verify instructions and maintain service records
- Improve our systems, processes and service delivery
- Protect our business, clients and systems from fraud, error and security threats

If we are unable to collect required information, we may not be able to provide some or all of our services.

6. Disclosure of Personal Information

We may disclose personal information where reasonably necessary to provide our services.

We only disclose personal information where:

- the client has authorised or permitted us to do so, including where relevant through our engagement arrangements;
- we have a legal duty to make the disclosure; or
- the disclosure is otherwise permitted by applicable law and is consistent with our professional obligations as a registered BAS Agent.

Where client permission is required under our professional obligations, we obtain that permission before making the disclosure.

Recipients may include:

- Our employees and authorised offshore team members located in Australia and the Philippines
- Software providers and cloud service providers
- Professional advisers
- Superannuation funds
- Financial institutions
- Government agencies and regulators
- The Australian Taxation Office
- The Tax Practitioners Board
- Law enforcement agencies where required by law

We do not sell personal information.

7. Overseas Disclosure of Personal Information

Some personal information may be accessed, processed or stored outside Australia.

This may occur because:

- Authorised Notch Above offshore team members located in the Philippines assist in delivering bookkeeping, payroll and administrative support services; and
- Certain software and cloud service providers operate infrastructure, support services or data centres outside Australia.

We take reasonable steps to ensure overseas recipients handle personal information consistently with Australian privacy obligations through contractual controls, access restrictions, confidentiality obligations and security measures.

8. Use of Artificial Intelligence (AI)

Notch Above uses approved AI-assisted technologies to improve efficiency, quality assurance, workflow management and service delivery.

Current examples include:

- ChatGPT Business
- XBert
- Vinyl AI Notetaker

These technologies may be used for:

- Quality assurance activities
- Procedure and SOP maintenance
- Meeting transcription and action tracking
- Administrative support
- Research and drafting assistance
- Workflow and compliance management

Notch Above has implemented controls governing the use of AI technologies.

ChatGPT Business

Staff must not enter client names, employee names, payroll records, bank account details or identifiable client financial information into ChatGPT Business.

Before client information is used in ChatGPT Business, it must be de-identified so that individuals are not reasonably identifiable.

Connected Bookkeeping and Transcription Tools

Approved connected bookkeeping tools, such as XBert, may process identifiable client information from accounting systems for transaction review and quality assurance.

Approved transcription tools, such as Vinyl AI Notetaker, may process identifiable information in client meeting recordings and transcripts to prepare meeting notes and action items.

These uses are subject to the disclosure permissions, access restrictions and security controls described in this Privacy Policy.

Human Review and Oversight

AI-generated outputs are reviewed by appropriately trained personnel before being relied upon in delivering our services.

We regularly review our use of AI technologies to ensure they remain appropriate, secure and consistent with our legal, professional and ethical obligations.

AI tools are used to assist human decision-making and do not replace professional judgement.

9. Storage and Security of Personal Information

We take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification and disclosure.

We regularly review and update our technical, administrative and physical security measures to respond to evolving cybersecurity risks, technological developments and changes to our legal and professional obligations.

Security measures include:

- Multi-factor authentication
- Role-based access controls
- Enterprise password and privileged access management (currently Practice Protect)
- Device security controls
- Secure cloud platforms
- Staff confidentiality obligations
- Restricted system permissions
- Cyber security monitoring
- Cyber insurance coverage
- Internal policies and procedures
- Data breach response processes

Access to personal information is limited to authorised personnel who require access to perform their duties.

10. Retention and Destruction of Information

We retain personal information for as long as reasonably necessary to:

- Provide our services;
- Meet taxation, bookkeeping and BAS Agent obligations;
- Comply with legal and regulatory requirements;
- Resolve disputes; and
- Protect our legitimate business interests.

We generally retain records for at least the periods required under applicable taxation, professional and legal obligations.

When information is no longer required, we take reasonable steps to securely destroy or de-identify it.

Depending on the nature of the information, this may include secure deletion of electronic records, secure destruction of physical documents or permanent de-identification of information so that individuals can no longer be identified.

10A. Tax File Numbers

In the course of providing payroll and related bookkeeping services, we may have access to Tax File Number (TFN) information relating to employees of our clients through authorised payroll systems.

We do not provide income tax return preparation services, collect clients' TFNs for that purpose, or require access to clients' income tax returns.

Where we receive or have access to TFN information, we only collect, record, use and disclose that information as permitted by applicable taxation and superannuation laws and the Privacy (Tax File Number) Rule 2015.

Access to TFN information is restricted to authorised personnel who require access to perform payroll or related bookkeeping duties, and security controls are applied to protect this information.

11. Website Information

At the date of this Privacy Policy, our website does not intentionally use analytics tools, advertising pixels or tracking technologies that collect personal information for marketing purposes.

If this changes in the future, we may update this Privacy Policy accordingly.

Information collected through website contact forms or enquiries will be handled in accordance with this Privacy Policy.

We also use reasonable technical and organisational security measures to protect information submitted through our website from unauthorised access, disclosure or misuse.

12. Direct Marketing

We do not currently engage in routine direct marketing activities.

If we send marketing communications in the future, recipients will be provided with an opportunity to unsubscribe or opt out where required by law.

13. Accessing and Correcting Personal Information

You may request access to personal information we hold about you.

You may also request correction of information that is inaccurate, incomplete, out-of-date, irrelevant or misleading.

Requests should be directed to the contact details below.

We may require verification of identity before granting access or making corrections.

In limited circumstances permitted by law, we may refuse access and will provide reasons where required.

14. Data Breaches

Notch Above maintains procedures for identifying, assessing and responding to data breaches.

Where a data breach is likely to result in serious harm, we will comply with our obligations under the Notifiable Data Breaches Scheme, including:

- Investigating the incident;
- Taking steps to contain and remediate the breach;

- Notifying affected individuals where required; and
- Notifying the Office of the Australian Information Commissioner (OAIC) where required by law.

15. Privacy Complaints

If you believe we have breached your privacy or mishandled your personal information, please contact us.

We will generally:

- Acknowledge your complaint within five (5) business days; and
- Seek to provide a substantive response within thirty (30) days.

If you are not satisfied with our response, you may be able to make a complaint to the Office of the Australian Information Commissioner (OAIC). Information about making a privacy complaint is available from the OAIC at oaic.gov.au.

16. Contact Us

Privacy Officer

Notch Above Bookkeeping Pty Ltd

PO Box 150
Paddington QLD 4064

Email: life@notchabove.com.au

Phone: 1300 015 130

17. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our business practices, technology, legal obligations or regulatory requirements.

The current version will always be available on our website.

We encourage clients and website users to review this Privacy Policy periodically.

People first. Technology enabled. Professionally accountable.